4a

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/083,236	02/26/2002	Craig L. Ogg	47187/RRT/S850	5848

23363 7590 04/10/2006

CHRISTIE, PARKER & HALE, LLP
PO BOX 7068
PASADENA, CA 91109-7068

EXAMINER	
HOMAYOUNMEHR, FARID	

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/083,236	**Applicant(s)** OGG ET AL.
	Examiner Farid Homayounmehr	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 February 2006*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-37* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communications: application, filed 2/26/2002; amendment filed 2/15/2006.

2. Claims 1 to 37 are pending in the case. Claims 1, 4, 22, 25, and 31 are amended.

Response to Arguments

3. Applicant's arguments filed 4/21/2005 have been fully considered but are not persuasive.

4. In view of the amendments, objection to claim 4 is withdrawn.

5. Applicant argues that Whitehouse (U.S. 6,005,945, the referenced prior art) does not include the limitations "a database remote from the user terminal for securely storing the private key and the public key in a user transaction data record assigned to the user", and "a server system remote from the user terminal and coupled to the computer network including a computer executable code for authenticating the user with the user transaction data record utilizing the stored private key in the database, wherein the private key assigned to the user is not stored in the client system".

To support this argument, the applicant points out to different portions of Whitehouse that indicate storage of some private keys on the client side.

However, Whitehouse teaches different private keys for different purposes. There are private keys for the purpose of protection of communications between the client and the server, and other private keys for the purpose of business transactions on behalf of the client with a postal authority computer. The private keys encrypting the communication between the client and the server are stored on the client, as described by parts of Whitehouse pointed out by the applicant. However, private keys used for authentication of the client to conduct business transactions on behalf of the client with postal authority computer (item 180 in Fig. 4 or Fig. 7) are not stored on the client side. Whitehouse clearly explains the distinction between keys for communication and keys for business transactions in column 9 line 11 to 31. In particular, Whitehouse points out that user sensitive information (related to business transactions) are stored on the server and never on the client side (see column 9 line 15 to 18).

Therefore, applicant's argument that Whitehouse private keys are stored on client side is moot with respect to the keys used for business transactions on behalf of the client. All claims remain rejected.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1, 22 and 15 to 17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claims 1 and 22 are amended and claims 15 to 17 are dependent on claim 1 which is amended.

7.1. Where applicant acts as his or her own lexicographer to specifically define a term of a claim contrary to its ordinary meaning, the written description must clearly redefine the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The phrase "authenticating the user with the user transaction data record assigned to the user utilizing the stored private key in the database" is used in claims 1 and 22. The accepted meaning of a private key is a secrete element in a cryptographic process that should not be revealed to any other party involved in the cryptographic process. In claims 1 and 22, the private key is used for user authentication, which is not the accepted way of using private keys. The phrase is indefinite because the specification does not clearly redefine the process of authentication using a private key. In the Remarks/Arguments section of the applicant action filed 2/15/2006, applicant points out page 7, line 10 to page 72 line 20, Fig. 5 as the section supporting the mentioned phrase. However, the mentioned section or figure does not provide any support or enablement for using a private key for authentication.

7.2. Claims 15, 16 and 17 recite the limitation "the cryptographic function" in the first paragraph. There is insufficient antecedent basis for this limitation in the claim. This has occurred when “a cryptographic function” was removed from claim 1 due to amendment.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

9. Claims 1 to 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Whitehouse (US Patent No. 6,005,945). The reference is included and identified as prior art in application Information Disclosure Statement.

9.1. As per claims 1 and 22, Whitehouse is directed to a system and method for providing public key infrastructure security (column 9 lines 32 to 35) in a wide area computer network (Fig. 4, column 7 lines 54 to 68) comprising: a user terminal (Fig. 4, *user interface*) coupled to the computer network (Fig. 4, as described in column 7 lines 54 to 68) including a client system (Fig. 4 item 104 and PCs); a private key, and a public key assigned to a user when the user registers with the system using the user terminal (Fig. 4, column 7 lines 54 to 68); a database remote from the user terminal for securely storing the private key and the public key in a user transaction data record assigned to the user (column 8 lines 23 to 62, particularly the encryption keys 164, and column 13 line 20 to 35, which shows each indicium includes a digital signature, and column 12 lines 38 and 39 that shows each digital signature is signed by user's private key); and a server system remote from the user terminal (Fig. 4, item 102 *secure central computer,* as described in column 8 line23) and coupled to the computer network (column 8 lines 63 to 65) including a computer executable code for authenticating the user with the user transaction data record assigned to the user utilizing the stored private key is the database, wherein the private key assigned to the user is not stored in the client system (column 12 line 57 to column 13 line 55, also note that the user private key used to sign the digital signature is never stored in the client system (see section 5 above)).

9.2. As per claim 2, Whitehouse is directed to the system of claim 1, further comprising a plurality of security device transaction data stored in the database, wherein each security device transaction data is related to a respective user (column 10 line 45 to column 11 line 30).

9.3. As per claim 3, Whitehouse is directed the system of claim 1, wherein the private key is encrypted when it is stored in the database (column 18 lines 50 to 56).

9.4. As per claim 4, Whitehouse is directed the system of claim 2, wherein a respective security device transaction data related to a user (Fig. 5A item 200, 202, 204 and 206) is loaded into a cryptographic device (the process that decrypts the message requests and digital signatures, as described in column 12 line 15 to column 13 line 15) when the user requests a service (Fig. 5A, item 200).

9.5. As per claim 5, Whitehouse is directed the system of claim 1, wherein the server system includes a cryptographic device to authenticate the identity of the user (column 12 lines 15 to 55) and verify that the identified user is authorized to assume a role and perform a corresponding operation. Whitehouse clearly specifies separate and distinguished operations (e.g. request for postal indicium, authentication key generation and distribution, user account maintenance and account balancing, indicium generation or validation, etc.) to be performed by separate entities. For example, a <u>user</u> can only perform a limited set of operations, such as requesting for postal indicium, and plays no role in system administration or management tasks such as key verification (performed by an <u>auditor</u>, as described in column 18 line 14 to 40), crediting or debiting accounts (performed by the secured central computer, column 12 line 65 to column 13 line 15), authentication key generation or distribution (performed by Postal authorities or agents, as described in column 19 line 14 to 30) or Postal Indicium validation (column 20 line 55 to column 21 line 19). Therefore, the examiner asserts that it discloses the feature.

9.6. As per claim 6, Whitehouse is directed the system of claim 5, wherein the assumed role is a security officer role to initiate a key management function (the key management function is performed by *the postal authority computer* as described in column 20 line 16 to 40).

9.7. As per claim 7, Whitehouse is directed the system of claim 5, wherein the assumed role is an administrator role to manage a user access control database (the management of user database is performed within the secure central computer, where it stores and protects user data as described in column 10 line 45 to column 11 line 12).

9.8. As per claim 8, Whitehouse is directed the system of claim 5, wherein the assumed role is a provider role to withdraw from a user account (the central computer performs the role of user account withdrawal as described in column 12 line 65 to column 13 line 15).

9.9. As per claim 9, Whitehouse is directed the system of claim 5, wherein the assumed role is a user role to operate on a value bearing item (the user role is performed by the user computer, requesting indicium, as described in Fig. 5A item 200).

9.10. As per claim 10, Whitehouse is directed the system of claim 5, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified (column 18, line 14 to 40).

9.11. As per claim 11, Whitehouse is directed the system of claim 5, wherein the cryptographic device (part of the *secured central computer*) includes a computer executable code for supporting multiple concurrent users and maintaining a separation of roles and operations performed by each user (column 20 line 55 to column 23 line 18).

9.12. As per claim 12, Whitehouse is directed the system of claim 5, wherein the cryptographic device stores information about a number of last transactions in a respective internal register (disclosed by the transaction log, column 9 lines 12 to 31).

9.13. As per claim 13, Whitehouse is directed the system of claim 12, wherein the database stores a table including the respective information about a last transaction (column 9 line 12 to 31), a verification module to compare the information saved in the device with the information saved in the database (column 20 line 52 to column 23 line 19).

9.14. As per claim 14, Whitehouse is directed the system of claim 1,further comprising a digital certificate stored in the database and assigned to a user when the user registers with the system (column 16 line 18 to column 17 line 35).

9.15. As per claim 15, Whitehouse is directed the system of claim 1, wherein the cryptographic function is digitally signing a certificate (column 10 line 45 to column 11 line 30).

9.16. As per claim 16, Whitehouse is directed the system of claim 1, wherein the cryptographic function is encrypting data (claim 1).

9.17. As per claim 17, Whitehouse is directed the system of claim 1, wherein the cryptographic function is decrypting data (claim 1).

9.18. As per claim 18, Whitehouse is directed the system of claim 1, wherein the database includes a user profile for the user (column 10 line 45 to column 11 line 10).

9.19. As per claim 19, Whitehouse is directed to the system of claim 18, wherein the user profile includes username, password, account expiration, user role, logon failure count, logon failure limit, logon time-out limit, password expiration, and password period (column 10 line 45 to column 11 line 15).

9.20. As per claim 20, Whitehouse is directed to system of claim 5, wherein the cryptographic device is capable of performing one or more of Rivest, Shamir and Adleman (RSA) public key encryption (clearly disclosed in column 16 line 39 to 45), DES (clearly disclosed in column 23 line 49 to 59), Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (which are comparable encryption algorithms to RSA (column 16 line 41) and obvious choices to a person skilled in the art to use as alternative methods of encryption).

9.21. As per claim 21, Whitehouse is directed to system of claim 5, wherein the cryptographic device stores information about a number of last transactions in an internal register (current piece count, column 10 line 64) and compares the information saved in the register with the information saved in a memory before loading a new transaction data (column 20 line 52 to column 22 line 51).

9.22. As per claim 23, Whitehouse is directed to the method of claim 22, further comprising the step of storing a digital certificate and assigning the stored digital certificate to a user when the user registers with the system (column 16 line 18 to column 17 line 35).

9.23. As per claim 24, Whitehouse is directed to the method of claim 22, further comprising the step of storing a plurality of security device transaction data in the database, wherein each transaction data is related to one of a plurality of users (column 10 line 45 to column 11 line 30).

9.24. As per claim 25, Whitehouse is directed the method of claim 24, further comprising the step of loading a security device transaction data related to a user (Fig. 5A item 200, 202, 204 and 206) into one of one or more of cryptographic devices (the process that decrypts the message requests and digital signatures, as described in column 12 line 15 to column 13 line 15) when the user requests to operate on a value bearing item (Fig. 5A, item 200).

9.25. As per claim 26, Whitehouse is directed the method of claim 25, further comprising the step of verifying that the requesting user is authorized to assume a role and to perform a corresponding operation. Whitehouse clearly specifies separate and distinguished operations (e.g. request for postal indicium, authentication key generation and distribution, user account maintenance and account balancing, indicium generation or validation, etc.) to be performed by separate entities. For example, a <u>user</u> can only perform a limited set of operations, such as requesting for postal indicium, and plays no role in system administration or management tasks such as key verification (performed by an <u>auditor</u>, as described in column 18 line 14 to 40), crediting or debiting accounts (performed by the secured central computer, column 12 line 65 to column 13 line 15), authentication key generation or distribution (performed by Postal authorities or agents, as described in column 19 line 14 to 30) or Postal Indicium validation (column 20 line 55 to column 21 line 19). Therefore, the examiner asserts that it discloses the feature.

9.26. As per claim 27, Whitehouse is directed the method of claim 26, wherein the assumed role is an administrator role to manage a user access control (the management of user database is performed within the secure central computer, where it stores and protects user data as described in column 10 line 45 to column 11 line 12).

9.27. As per claim 28, Whitehouse is directed the method of claim 26, wherein the assumed role is a user role to perform expected IBIP postal meter operations (column 25 line 45 to column 26 line 10).

9.28. As per claim 29, Whitehouse is directed the method of claim 26, wherein the assumed role is a certificate authority role to allow a public key certificate to be loaded and verified (column 18, line 14 to 40).

9.29. As per claim 30, Whitehouse is directed the method of claim 26, further comprising the steps of supporting multiple concurrent operators and maintaining a separation of roles and operations performed by each operator (column 20 line 55 to column 23 line 18).

9.30. As per claim 31, Whitehouse is directed the method of claim 25, further comprising the steps of: storing information about a number of last transactions in a respective internal register of each of the one or more cryptographic devices; storing a table including the information about a last transaction in the database (column 9 line 12 to 31); comparing the information saved in the respective device with the respective information saved in the database; and loading a new transaction data if the respective information stored in the device compares with the respective information stored in the database (column 20 line 52 to column 23 line 19).

9.31. As per claim 32, Whitehouse is directed the method of claim 22, wherein the cryptographic function is digitally signing a certificate (column 10 line 45 to column 11 line 30).

9.32. As per claim 33, Whitehouse is directed the method of claim 22, wherein the cryptographic function is encrypting data (claim 1).

9.33. As per claim 34, Whitehouse is directed the method of claim 22, wherein the cryptographic function is decrypting data (claim 1).

9.34. As per claim 35, Whitehouse is directed the method of claim 22, further comprising the step of storing a user profile for a plurality of users (column 10 line 45 to column 11 line 10).

9.35. As per claim 36, Whitehouse is directed the method of claim 35, wherein the user profile includes username, user role, password, logon failure count, logon failure limit, logon time-out limit, account expiration, password expiration, and password period (column 10 line 45 to column 11 line 15).

9.36. As per claim 37, Whitehouse is directed the method of claim 22, wherein the cryptographic function is one or more of Rivest, Shamir and Adleman (RSA) public key encryption (clearly disclosed in column 16 line 39 to 45), DES (clearly disclosed in column 23 line 49 to 59), Triple-DES, DSA signature, SHA-1, and Pseudo-random number generation algorithms (which are comparable encryption algorithms to RSA (column 16 line 41) and obvious choices to a person skilled in the art to use as alternative methods of encryption).

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farid Homayounmehr whose telephone number is (571) 272-3937. The examiner can be normally reached on 9 hrs Mon-Fri, off Monday biweekly.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Farid Homayounmehr

11/1/2005

Gilberto Ba

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100